NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/reviews/2012/021312-ipv6-application-delivery-controllers-test-255474.html

IPv6 deployment starts at the network edge

Six ADCs deliver IPv6 capabilities to apps hosted on IPv4 Web servers

By Scott Hogg, Network World
February 13, 2012 12:08 AM ET

IT execs know they will have to deploy IPv6 at some point, but where to begin? One approach that establishes some IPv6 capability without spending a lot of time or money is to start at the perimeter.

IPv6-enabling routers, firewalls and DNS servers should be straightforward. If an organization were to deploy an IPv6-capable Server Load Balancer (SLB) or, using the most current term, Application Delivery Controller (ADC), they could configure an IPv6 Virtual IP (VIP) and an IPv4-only server farm.

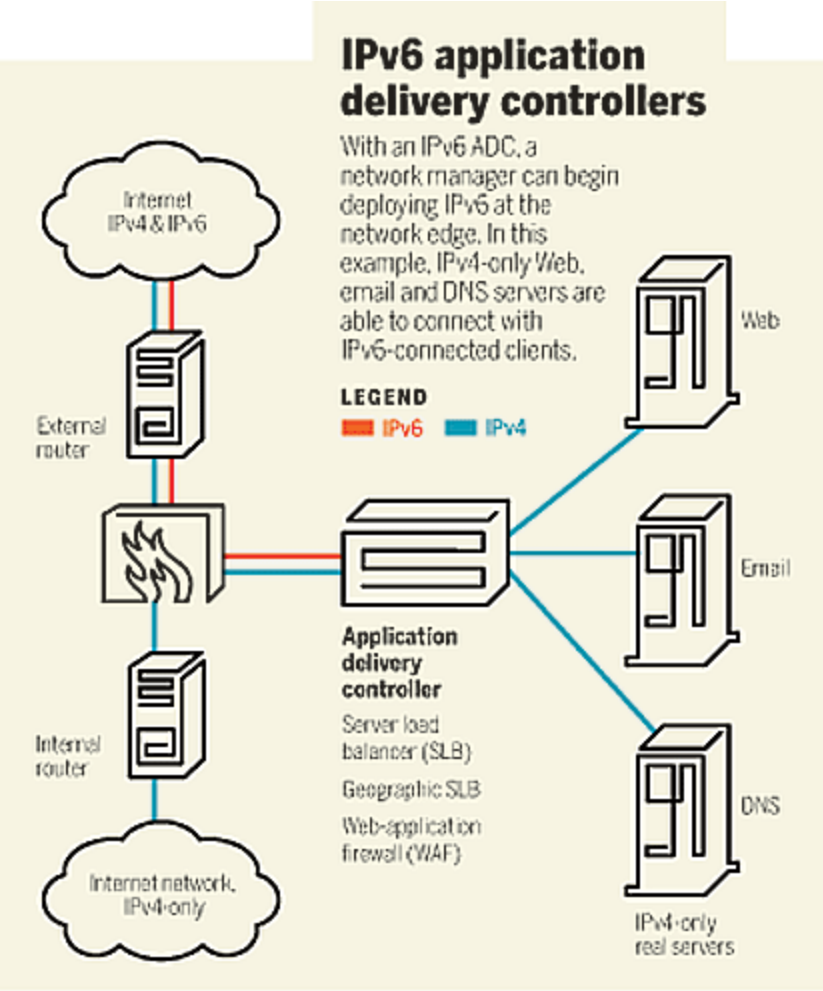
This would allow Web apps hosted on IPv4-only servers to appear to the Internet user as IPv6-applications. The way it works is that clients would connect to the IPv6 VIP, and the ADC would perform a reverse-proxy function and terminate the IPv6 HTTP Internet connection, then create a new IPv4 HTTP back-end connection to the IPv4-only application servers. The server would not necessarily know the IP version being used by the client and it would happily return the data to the ADC appliance using IPv4. The ADC appliance takes that IPv4 response from the server, copies the HTTP application data and transmits it back to the IPv6-connected client.

Quiz: are you ready for IPv6?

We tested the IPv6 capabilities of the major ADC vendors' products: A10 Networks, Brocade, Cisco, Citrix, F5 and Riverbed/Zeus. We tested all of the IPv6 features that these vendors listed on their data sheets and determined that all of these systems are suitable for aiding in an Internet edge IPv6 deployment scenario.

IPv6: What you need to do now

One piece of good news: The ADC your company already owns may have IPv6 capabilities. It could be as simple as a software upgrade and you would have an IPv6-capable reverse proxy server that could help accelerate your IPv6 Internet edge deployment.



Click to see: IPv6 diagram

Long list of features

ADCs can provide a wide variety of IPv6 capabilities. Most of the products tested had these features.

• IPv4/IPv6 Server Load Balancing (reverse proxy), IPv6 VIP with IPv4 or dual-protocol real-servers/server-farms

• SSL offload and acceleration for IPv6-VIPs and servers

• Ability to perform content filtering, regular expression matching, URL rewriting, for IPv6 connections

• IPv6-capable Web Application Firewall (WAF)

• IPv6-enabled security features (distributed denial-of-service (DoS) protection, SYN-cookies, IPS, content filtering)

• Stateful access control lists f(ACL) or IPv6 packets, ICMPv6 filtering, extension header filtering and denial of RH0 packets

• High-availability for IPv6 connections (IPv6 connection state synchronization between high availability pairs)

• Logging of IPv6 connections (internal logging and with Syslog)

• Ability to check the IPv6 neighbor cache entries

• IPv6 static routing

There are also some nice-to-have optional features.

• IPv6-enabled Geographical Server Load Balancing (GSLB)

• Authoritative dual-protocol DNS server

• Stateful NAT64 capabilities

• DNS64 integration with NAT64

• IPv6 routing protocol support (static routing, RIPng, OSPFv3, IS-IS [ST & MT], MP-BGP, RHI)

• Management with IPv4 and IPv6

There are also IPv6 features that apply to ISPs or large-scale data center companies.

• Large Scale NAT (LSN), Carrier Grade NAT (CGN), NAT444

• 6rd (IPv6 Rapid Deployment) border relay

• Dual-Stack Lite (DS-Lite) AFTR

Many of these features have crept into ADC products over several years. Some are included as part of the base licensing, but be aware that some vendors may charge a premium for these IPv6 features.

We set up a testing environment that mimicked a typical Internet edge environment. We had an IPv4-only perimeter and we enabled it for IPv6. We performed testing from the perspective of an IPv6-enabled Internet user trying to establish connectivity to an IPv4-only web server. We also tested NAT64 functionality where an IPv6-only client may be trying to reach IPv4 Internet content.

We tested each of these six ADCs and found that they were all capable of basic IPv4 and IPv6 server load balancing with SSL offload. We found that the support for IPv6 management, IPv6 routing, and service-provider IPv6 features varied quite widely among the vendor's solutions. We found that all of these products would be suitable in an enterprise Internet perimeter environment and would aid in the transition to IPv6.

FEATURESCOMPARISON

Company	A10 Networks	Brocade	Cisco	Citrix	F5	Riverbed
Product	AX 2500 Version 2.6.1 and 2.6.6	ADX 1216-4-SSL-PREM	ACE-4710-01-K9 Version A5 (1.1)	Net Scaler MPX7500 Version 9.3-5.2.3	F5-BIG-3900-E-R Version 11.1	Stingray 4000 VH Version 8.0r0
Price	$24,995	$45.995	$29,995	$22,000	$52,995 plus $23,990	$63,000
6-to-6, 6-to-4 SLB	Yes	Yes	Yes	Yes	Yes	Yes
SSL offload	Yes	Yes	Yes	Yes	Yes	Yes
NAT64/DNS64	NAT64 and DNS64 — Infoblox	NAT64 but no DNS64 — Secure64	No	No	No	No
IPv6 GSLB	Yes	Yes	No — GSS 4492 separate product	Yes	Yes	Yes
IPv6 WAF	No	No	No	Yes	Couldn't test it	No
LSN/DS-Lite/6rd	Yes	LSN but no DS-Lite or 6rd	No	No	No	No
IPv6 routing	Yes	Yes	No	No	No	No
IPv6 mgmt.	Yes	Yes	No	Yes	Yes	No
Installation	5	4	5	4	3	5
Feature set	5	4	2	4	4	3
Manageability	5	5	4	4	3	5

Click to see: IPv6 chart of products
Scariest IPv6 attack scenarios

Here are the individual reviews:

A10 Networks AX2500: Highly scalable, feature rich, lacks web app firewall

A10 first started supporting IPv6 in their AX series in 2007. Since then, A10 has fully embraced IPv6. Today, A10 offers two version of their software: one (2.6.1) for IPv6 SLB and one (2.6.6) for NAT64/DNS64 /DS-Lite/6rd and Large Scale NAT (LSN), also known as CGN or NAT444 (IPv4 preservation).

A10 also has a SoftAX virtual appliance for lab or production environments. We tested an AX2500 which lists for $24,995, however, A10 has appliances that range from $15,995 to $215,000 and their SoftAX virtual appliance can cost between $995 and $24,995. The great thing is that all the AX features are included without additional license fees.

The A10 Networks AX series of ADCs have many IPv6 features including IPv4/IPv6 SLB with SSL offload and GSLB over IPv6. The AX can perform Syslog for IPv6 connections using aFleX Tcl scripts. The AX also allows Ping and management access using SSH, HTTP/HTTPS, SCP and SFTP over IPv6 transport.

Unfortunately, there are no IPv6 WAF capabilities in this version, but A10 appliances can integrate with other market-leading WAFs such as Imperva. We found that the A10 does provide other security features like protocol checking for HTTP, HTTPS, and DNS, distributed DoS protections, rate limiting, and ACLs.

Our testing determined that A10 supports static IPv6 routes and dynamic routing protocols for IPv6. The A10 can be configured for RIPng, OSPFv3, IS-IS and BGP.

A10's SoftAX virtual appliance can help support an organization's cloud computing and virtualization goals. The A10 AX appliances also support multi-tenancy and virtual chassis configurations.

AX appliances have extensive scalability due to their 64-bit architecture and their Advanced Core Operating System (ACOS). However, scalability may not be a concern for enterprises who may initially have low IPv6 traffic volumes.

The A10 Networks systems also provide service-provider features such as NAT64 and DNS64. The 2.6.6 software can be configured for NAT64 with DNS64, but there is also a documented Infoblox integration of

DNS64 for A10's NAT64 configurations. The Large Scale NAT (LSN), DS-Lite, 6rd, NAT64/DNS64 scalability of these appliances makes them attractive to service providers. In fact, the A10s compete well with more costly heavy-iron solutions from the large router vendors.

Brocade ServerIron ADX: Newly updated software deliver rich feature set, but no Web app firewall

Brocade acquired Foundry Networks in 2008 and Brocade has continued innovating its routers, switches, and server load balancers. Brocade first starting adding IPv6 features to the ServerIron ADX platform in Version 11.0 and has continued to add IPv6 features to this ADC. We tested a Brocade ServerIron ADX 1216-4-SSL-PREM running Version 12.3.1 and the latest software Version 12.4.00T405 which has a list price of $45,995.

This system has the Premium License which includes Layer 3 Routing, IPv6, GSLB and an additional license for SSL offload. Brocade very recently came out with this new software that adds to the number of available IPv6 features. One item of note is that Brocade has a "pay-as-you-grow" licensing model and licenses the ADXs based on the software features, number of processors and bandwidth you require. Therefore, to get IPv6 capability on the ADX you must purchase the Premium License.

The ADX supports IPv4 and IPv6 Server Load Balancing as a reverse proxy server. VIPs can use either IPv4 or IPv6 addresses and have either IPv4 or IPv6 real servers. Brocade has completely rewritten their IP stack to accommodate and streamline IPv6. However, our testing revealed that their system only supports SSL offload for IPv4 VIPs using IPv4 real servers or IPv6 VIPs using IPv6 real servers. In software release 12.4, the ADX will be able to perform SSL offload for IPv6 VIPs using IPv4 real servers and mixed protocol server farms.

We set up the ADX and configured web management over IPv6 and we also entered IPv6 addresses into the configuration through the web GUI. We used SSH over IPv6 transport and SNMP worked over IPv6. Syslog did not work for IPv6 Syslog servers but IPv6-related log messages can be sent to an IPv4 Syslog server.

The ADX also supports a wide variety of IPv6 routing protocols including OSPFv3, IS-IS (Single-Topology or Multi-Topology) and MP-BGP.

The ADX offers IPv6 security features and allows you to configure complex IPv6 access-lists. The ADX now supports SYN-Proxy (SYN-cookies) for IPv6 traffic and setting the MSS works for IPv4 or IPv6 packets. We found that other features such as distributed DoS protection, IPS, and content filtering are also IPv6-capable. However, the Brocade ServerIron does not have an IPv6-capable WAF.

The ServerIron ADX can act as an authoritative dual-protocol DNS server, function as a DNS proxy server and perform IPv4 and IPv6 GSLB.

The Brocade ADX supports NAT64 in the same software and hardware, but it is configured in a different operating mode from traditional SLB functions. Our testing determined that you cannot have a single ADX appliance function as a NAT64 system and a server load balancer at the same time.

The ADX has capabilities for IPv6-only or IPv4-only clients. The Brocade ServerIrons can perform Large Scale NAT (LSN)/Carrier Grade NAT (CGN)/NAT444, but do not currently support 6rd or DS-Lite.

Cisco ACE A5: Late to the IPv6 party, features are somewhat limited

The Cisco Application Control Engine (ACE) has been available for many years in many forms but only a few months ago did the Cisco ACE begin to support IPv6. ACE software release A5 (1.1) runs on the ACE30

module for a Cisco 6500 switch and the ACE4710 appliance. Unfortunately, customers who have invested in ACE10 or ACE20 modules will not be able to use this version and will face hardware upgrades to support IPv6. There are ACE10/20 to ACE30 upgrades available for $30,000. The device that we tested was the ACE-4710-01-K9 running software Version A5 (1.1) which has a list price of $29,995.

Cisco ACE modules and appliances have licensing that allows the upgrade of the performance of the units, the number of SSL connections and number of virtual contexts. There is no additional charge for IPv6 support on the ACE. If you are familiar with configuration of Cisco devices using contexts then you will feel right at home with this system.

The Cisco ACE performed server load balancing for IPv6 VIPs with IPv6 real servers and IPv6 VIPs with IPv4 real servers. We easily configured IPv6 health probes and the Layer-4/Layer7 policies and SSL offload work for IPv6 connections. HTTP/HTTPS and DNS inspection (application awareness) work for native IPv6-IPv6 traffic. The ACE allowed us to configure IPv6 ACLs and perform packet capture of IPv6 packets. The ACE has IPv6 security features and it can filter extension headers, perform fragmentation inspection, IPv6 ICMP-guard, IPv6 normalization, and IPv6 Unicast-RPF checking. The ACE can act as a DHCPv6 relay and can either send Routing Advertisements on its Ethernet interfaces or suppress them. In the ACE, fault tolerance is not supported over IPv6 but it can track IPv6 connectivity and use IPv6 alias addresses on its interfaces.

The ACE does have some limitations. It does not support IPv6 dynamic routing protocols, but it does have IPv6 static routing and IPv6 Route Health Injection (RHI). The ACE does not have stateful NAT64 with or without DNS64. We could not configure IPv6 transport for management protocols (SSH, Telnet, SNMP, HTTP/HTTPS) but IPv6 MIB values are available for SNMP query over IPv4 transport.

We were able to perform IPv6 configuration through the web GUI, but it is only accessible over IPv4. We could ping the ACE using ICMPv6 and could send syslog messages with IPv6 addresses in them. The ACE GSS 4492 does have IPv6 support for GSLB. However, in August, Cisco announced end of sales for their ACE Web Application Firewall (WAF) so it will never be IPv6-capable.

Citrix NetScaler: Fully featured, easy to configure

NetScaler has supported IPv6 for more than seven years. IPv6 capabilities are available in the platinum, enterprise, and standard edition feature sets and now IPv6 comes enabled by default for no additional cost. We tested using a Citrix NetScaler MPX7500 running software Version 9.3-52.3 that costs $22,000. In addition to Citrix's hardware appliances, the company offers a virtual appliance called the NetScaler VPX.

It was easy to configure IPv6 addresses on interfaces and VLANs through either a command line interface (CLI) or the GUI. The Netscaler supports configuring IPv6 VIPs with IPv6 or IPv4 services. SSL offload worked for IPv6 and health probes operate over IPv6. Content switching worked for IPv6 connections and regular expressions could be created using IPv6 addresses. URL rewriting also worked for IPv6 VIPs. We could configure IPv6 for RADIUS servers, TACACS+ servers, LDAP servers, Syslog servers, and DNS servers.

The NetScaler can be an authoritative DNS server for IPv6 AAAA address records, which is important for the GSLB functionality. IPv6-capable DNS services helps make GSLB work for IPv6 addresses. High Availability could also use IPv6 addresses. We could create traffic filters that contain IPv6 addresses and IPv6 ACLs were easy to configure. We could manage the NetScaler over IPv6 transport and there are IPv6-specific MIBs/OIDs for the NetScaler that we could query over IPv6 SNMP. We were also able to create custom log formats using IPv6 source/destination addresses and v-server address.

The built-in web application firewall helps secure IPv4 and IPv6 services from attacks. Policies can be

created and applied to IPv6 applications just as easily as for IPv4 applications. The NetScaler software allows for the configuration of static IPv6 routes, and we also configured OSPFv3 and RIPng in the IP Infusion ZebOS Cisco-Like Interface. The NetScalers have IPv6 NAT (Inbound Network Address Translation (INAT) and prefix-translation capabilities. The NetScalers also support NAT64 and DNS64. The Citrix NetScaler also has IPv6 SSL VPN "Access Gateway" services.

F5 Big-IP: Full features, easy to customize

F5 has supported IPv6 in its BIG-IP ADC products for several years. The device we tested was the BIG-IP 3900 Local Traffic Manager Enterprise Edition, which has a list price of $52,995. This unit also includes the Global Traffic Manager module, for an additional $23,990. We tested using BIG-IP software version 11.1.0 Build 1943.0. The F5 hardware architecture combines x86_64 processors and FPGAs/network processors to provide performance and flexibility.

It was relatively easy to configure the unit with IPv6 addresses for Self-IPs. It was easy to use the GUI to configure IPv6 VIPs for IPv4 or IPv6 application servers. F5 supports IPv6 static and dynamic routing through the IP Infusion ZebOS configuration CLI although we had difficulties getting router adjacencies configured. The BIP-IP supports Route Domains (like virtual routers) and Administrative Partitions (multi-tenancy) and virtual Clustered Multi-Processing (vCMP) (running different software versions simultaneously on their chassis hardware).

The documentation mentioned that you must configure radvd for IPv6 support. However, we found that you do not need to configure radvd unless you need the BIG-IP to act like a default gateway router. In other words, if you want computers that are directly connected to the F5 hear the Router Advertisement ICMPv6 messages from the F5 then you must configure radvd through CLI to get IPv6 to function.

We configured the web management interface to use over either IPv4 or IPv6 but it cannot do both simultaneously. The self-IPs were reachable using IPv6 and SSH, and the F5 did allow for remote management of the system using IPv6 using SNMP v1/v2c/v3.

One of the powerful features of F5 LTMs is the iRules event-drive scripting language that allows the administrator to customize how application traffic is handled. iRules can be configured for matching on IPv6 addresses.

The latest version 11.1 now has IPv6 support for the Application Security Manager (WAF). This operating mode on the BIG-IP hardware should provide http protocol inspection to protect IPv6 web applications, however, we were not able to get this configured.

F5 also sells a virtual appliance called the BIG-IP Local Traffic Manager (LTM) Virtual Edition (VE) which can be an IPv6 load balancing gateway with NAT64/DNS64 support.

Riverbed Stingray Traffic Manager: East to setup, some IPv6 features lacking

Zeus Technology, which has been in business since 1995, released a virtual ADC appliance in 2004 and added IPv6 support to Zeus Traffic Manager in 2008. Last year Riverbed acquired Zeus and now the virtual ADC system is called the Stingray Traffic Manager.

Stingray Traffic Manager Version 8.0 was released on Oct. 25, 2011, with Version 4.1 of the Stingray Application Firewall now built into the Traffic Manager software distribution. Pricing for the Riverbed Stingray Traffic Manager 8.0 starts at $5,500 and goes up to $63,000 for the 4000VH, which is the unit we tested.

The Stingray Traffic Manager was very easy to set up as a Virtual Machine (VM). Nothing needed to be configured on the CLI of the virtual appliance. The only time we used the CLI was to gracefully shutdown the system. All other administrative tasks were performed with a web browser to connect to the management interface IP address.

Configuration was very simple and in just a few clicks we had IPv4-to-IPv4, IPv6-to-IPv6, or IPv6-to-IPv4 load balancing configured. The interface is intuitive enough that you may even be able to resist the urge to read the manual and still configure it successfully. It was trivially easy to configure IPv4 and IPv6 front end and back-end servers and services and IPv6-enabled SSL offload. Anywhere we could configure an IPv4 address we could configure an IPv6 address instead. We found that if we configured a full qualified domain name (FQDN), then it performed an IPv4 DNS lookup first, but if that fails then it used the IPv6 address returned by DNS. The Stingray Traffic Manager does not support stateful NAT64 but it does function as a proxy for IPv4 and IPv6 connections. Stingray Traffic Manager Version 8.0 does not support IP transparency for IPv6 back-ends or clients.

The Stingray supports TrafficScripts, which can be used for advanced traffic handling or for preventing distributed DoS attacks. We even successfully tested the Stingray Traffic Manager ZeusBench, which is a built-in IPv4/IPv6 traffic/server testing system. We found that information exchanged between traffic managers or clusters is done over IPv4 and heartbeat messages use only IPv4 packets.

The Stingray Application Firewall, the Application Firewall Module (AFM), does not currently support IPv6. Also the GSLB Multi-Site Manager (MSM) lacks IPv6 capabilities. The Zeus Traffic Manager cannot run a dynamic routing protocol like OSPFv3, but this is in development and should be available pretty soon.

Conclusions

The fact is that an IPv6-enabled Internet already exists and the transition to IPv6 is already underway in the U.S. government and other parts of the world. Much of your IPv6 Internet-perimeter infrastructure is already IPv6 capable. Regional Internet Registries have IPv6 addresses to give you, and your ISP may already have IPv6 Internet connectivity ready for you.

Use of an IPv6-capable reverse proxy server that could help accelerate your IPv6 Internet edge deployment. If you already own one of these systems and it is already deployed at your Internet perimeter or DMZ, you have very little capital expenditure to get your organization's web applications to be reachable with IPv6.

If you own an ADC that does not have IPv6 capabilities then it would be worth speaking to your vendor to see when they may have such features. However, if your vendor has not put IPv6 on their product development roadmap at this stage, then you are likely to be purchasing a new system to gain this functionality. Any of the six products in this test will fit the bill.

Hogg is Director of Technology Solutions at GTRI, Chair of the Rocky Mountain IPv6 Task Force, and author of a Cisco Press book on IPv6 Security. He can be reached at scott@hoggnet.com

Read more about lans & wans in Network World's LANs & WANs section.